



CVE-2023-20842

Published on: Not Yet Published

Last Modified on: 09/07/2023 02:38:00 PM UTC

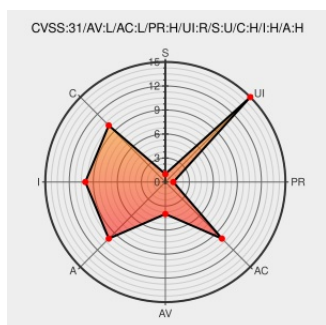
CVE-2023-20842

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Android](#) from [Google](#) contain the following vulnerability:

In `imgsys_cmdq`, there is a possible out of bounds write due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07354259; Issue ID: ALPS07340477.

CVE-2023-20842 has been assigned by [security@mediatek.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [MediaTek, Inc.](#) - MT2713, MT6895, MT6897, MT6983, MT8188, MT8195, MT8395, MT8781 version = **Android 11.0, 12.0 / Linux 6.1 / IOT-v23.0 / Yocto 4.0**

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
September 2023	corp.mediatek.com text/html	MISC corp.mediatek.com/product-security-bulletin/September-2023

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	11.0	All	All	All
Operating System	Google	Android	12.0	All	All	All
Operating System	Linux	Linux Kernel	6.1	-	All	All
Application	Linuxfoundation	Yocto	4.0	All	All	All
Application	Mediatek	Iot Yocto	23.0	All	All	All
Hardware 🚢🔗	Mediatek	Mt2713	-	All	All	All
Hardware 🚢🔗	Mediatek	Mt6895	-	All	All	All
Hardware 🚢🔗	Mediatek	Mt6897	-	All	All	All
Hardware 🚢🔗	Mediatek	Mt6983	-	All	All	All
Hardware 🚢🔗	Mediatek	Mt8188	-	All	All	All
Hardware 🚢🔗	Mediatek	Mt8195	-	All	All	All
Hardware 🚢🔗	Mediatek	Mt8395	-	All	All	All
Hardware 🚢🔗	Mediatek	Mt8781	-	All	All	All
cpe:2.3:o:google:android:11.0:*:*:*:*:*:						
cpe:2.3:o:google:android:12.0:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:6.1:-:*:*:*:*:						
cpe:2.3:a:linuxfoundation:yocto:4.0:*:*:*:*:*:						
cpe:2.3:a:mediatek:iot_yocto:23.0:*:*:*:*:*:						
cpe:2.3:h:mediatek:mt2713:-:*:*:*:*:						
cpe:2.3:h:mediatek:mt6895:-:*:*:*:*:						
cpe:2.3:h:mediatek:mt6897:-:*:*:*:*:						
cpe:2.3:h:mediatek:mt6983:-:*:*:*:*:						
cpe:2.3:h:mediatek:mt8188:-:*:*:*:*:						
cpe:2.3:h:mediatek:mt8195:-:*:*:*:*:						
cpe:2.3:h:mediatek:mt8395:-:*:*:*:*:						
cpe:2.3:h:mediatek:mt8781:-:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)